The way ahead to Voice Over Internet Protocol (VOIP) in DoD – Convergence or Non-Convergence

Dr. Eugene W.P. Bingue

IT Planner, NCTAMS-PAC, Wahiawa, Hawaii

Eugene.Bingue@navy.mil

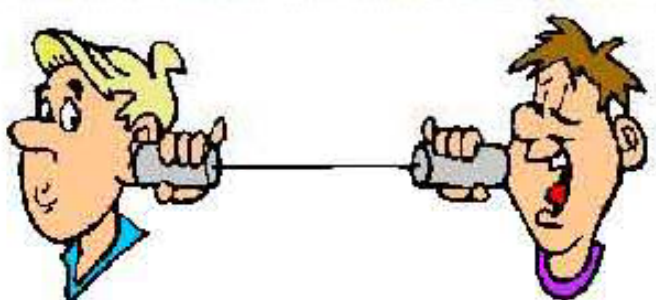
Dr. David A. Cook

Senior Research Scientist and

Principal Member of the Technical Staff

The AEgis Technologies Group, Inc. Albuquerque, NM

dcook@aegistg.com



Objectives

- Introduction
- JITC and Command & Control issues
- VOIP desktop solution alternatives
- Enterprise architectures convergence
- The next step – planning the move

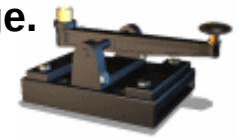
Introduction

- VOIP is becoming the smart way to embrace expanding broadband technology.
- Alexander Graham Bell's telephone of 1876 has evolved over two centuries to become an integral part of DoD's operations providing incidental communication to command and control of some of the most lethal arsenal on earth.
- Does VOIP change the paradigm of telephony in the 21st century?
- And, if so – how do we adapt to IP Telephony (IPT)?

Introduction
Why VOIP

1539 - Mexico began using the first printing press in the Western Hemisphere.

1844 - Samuel Morse transmitted the first public telegraph message.

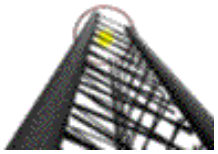


1858 - The first Transatlantic cable was laid

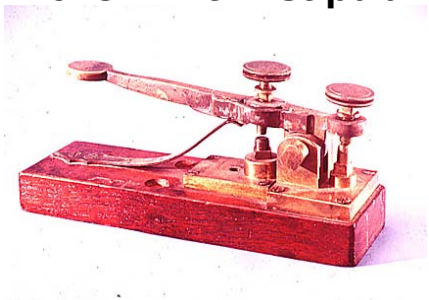
1876- Alexander Graham Bell invented the telephone in Boston in 1876, 120 years later there are over 360 million telephone numbers, and that figure grows each year.

1906 - First wireless communication of human speech.

1936 - First television broadcast made in London, England.



1973 - The first public telephone call placed on a portable cellular phone.



The telegraph key Samuel Morse used on his first line in 1844

FEB 2009

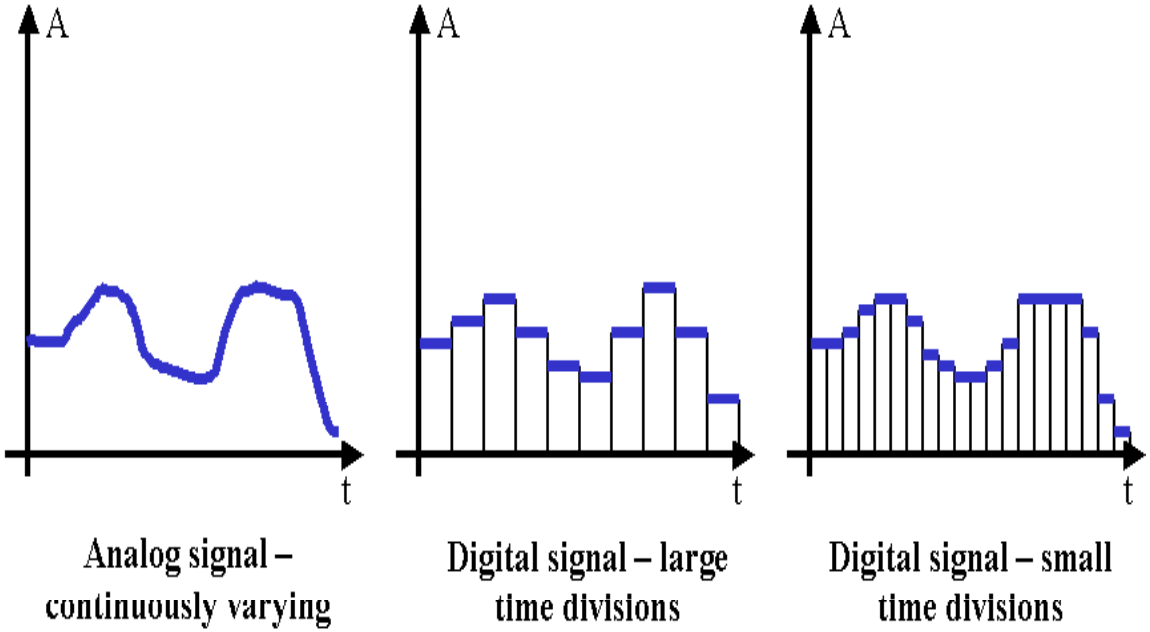
Martin Cooper demonstrates the first portable cellular telephone. ArrayComm

Introduction
Analog to Digital

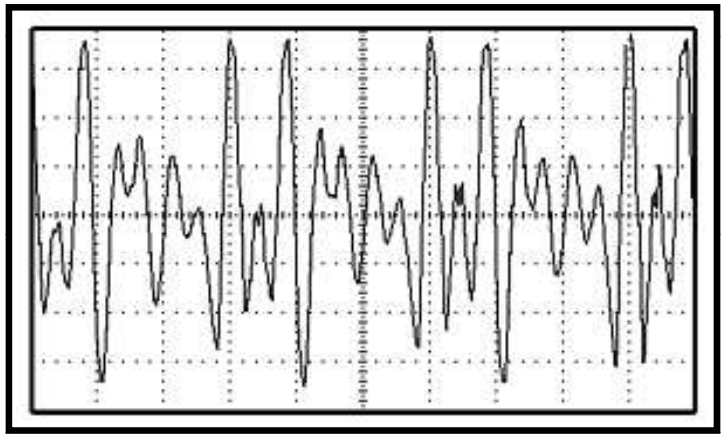
Time Division Multiplexing (TDM) network that dedicates channels and reserves bandwidth as needed out of the trunk links: Circuit switching

IP networks are different from circuit-switching, in that it is a packet-network, based on statistical availability.

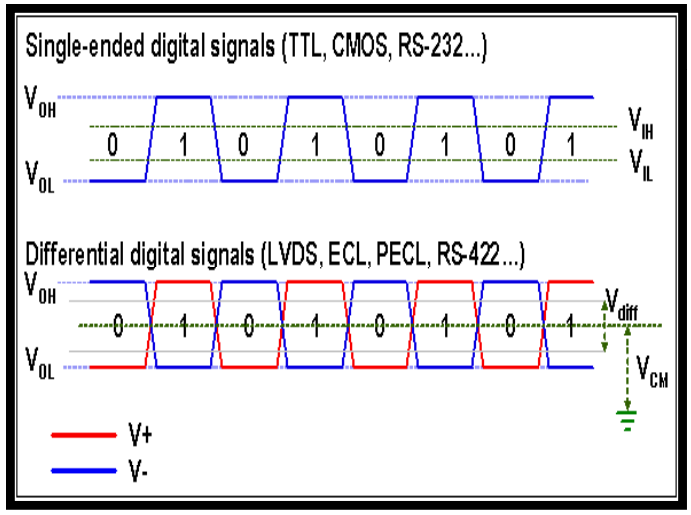
Class of service (CoS) ensures that packets of a specific application are given priority.



Analog Signal-Voice



Digital Signal-Data

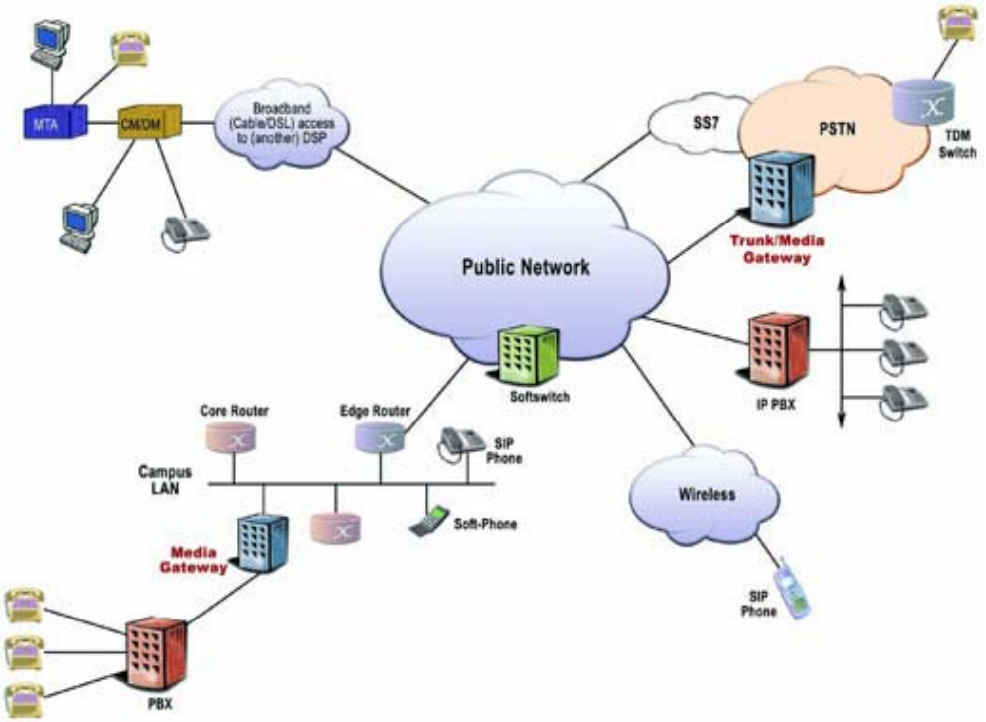


Introduction

DISA “Network Centric Warfare”

- Voice Over Internet Protocol (VoIP) is an emerging technology that is a critical component of network centric warfare.

- All major common carriers and telecommunications switch vendors plan to migrate to VoIP. As they migrate, their support to DSN circuit switches will diminish.



- VoIP is a critical step toward DoD's ability to effectively provide all DoD communications traffic (data, voice, video, etc.) on an IP network. This is the key concept to effective Net Centric warfare

Introduction

DISA "Network Centric Warfare"

- The Joint Chief of Staff (JCS) Military Communications Electronics Board (MCEB) endorsed three near-term major operational drivers for the introduction of VoIP services to support network centric warfare:
  - **Convergence** of secure desktop services at major command centers is driving the need for VoIP service on the SIPRNet and gateways to the DRSN
  - **Small footprint** and highly mobile tactical deployments are driving the need for tactical extensions via both SIPRNet and DSN gateways
  - **Investment** many Military Departments and Agencies have deployed VoIP systems at the edge of the DSN as on-base intercoms and as pilots

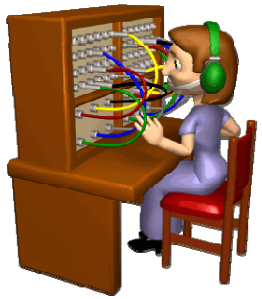
JITC and Command & Control issues
DISA

- JITC provides a full-range of agile and cost-effective test, evaluation, and certification services to support rapid acquisition and fielding of global net-centric warfighting capabilities.

JITC and Command & Control issues

TSSI

- The Telecom Switched Services Interoperability (TSSI) Program includes interoperability certification of DOD's voice, video, and data services across the circuit switched network.
- The circuit switched network comprises the Defense Switched Network (DSN) and customer premise equipment (CPE).
- As approved by Office of the Secretary of Defense (OSD), the DSN, is an interbase, nonsecure or secure Command & Control (C2) telecommunications system that provides end-to-end command use and dedicated telephone service, voice-band data, and dial-up video teleconferencing (VTC) for C2 and non-C2 DOD authorized users in accordance with national security directives.
- Non-secure dial-up voice (telephone) service is the system's principal requirement.



JITC and Command & Control issues

General and Military-Unique Requirements

The DSN must adhere to the capability objectives below to ensure its ability to support effective military C2 functions.

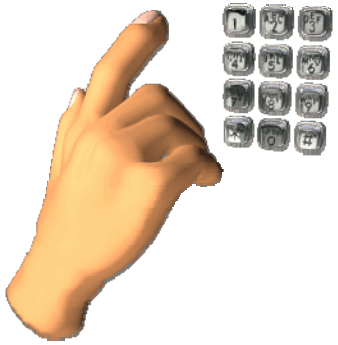
- **Survivable Service**. DSN supports C2 user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions and possesses the robustness to provide a surge capability when needed. System robustness through maximum use of alternative routing, backup, etc.
- **Assured Connectivity**. DSN is required to provide assured voice communications to C2 users. Assured service or connectivity is defined as the ability of the DSN to optimize call completion rates for all C2 users in accordance with the guidelines in this instruction, despite degradation because of network disruptions, natural disasters, or surges during crisis or war. The DSN was designed with military-unique feature (MUF) requirements such as multi-level precedence and preemption (MLPP). MLPP permits higher precedence users to preempt lower precedence calls. Special C2 users (FLASH and FLASH OVERRIDE within the current DSN MLPP framework) are provided with nonblocking service (P.00 threshold) from user to user. (P.00 = out of every 100 calls, the probability is that zero calls will be blocked.

JITC and Command & Control issues

General and Military-Unique Requirements (con't)

- **Responsive Service.** DSN service must be responsive to the needs of C2 users. Special C2 users under current DSN MLPP scheme -- FLASH and FLASH OVERRIDE -- are provided nonblocking service.
- **Surge Capacity**. Mitigation of short-term traffic surges is inherent in the MLPP capabilities of the DSN. DISA will ensure that PRIORITY and IMMEDIATE traffic will encounter, at a minimum, GOS of P.02 (two calls out of 100 will be "blocked" during the "busy hour") and P.01 respectively during a 100 percent increase above normal precedence usage.

- **Secure Service**. DSN permits, through the use of secure instruments, protection of classified and sensitive information being passed, to ensure its confidentiality, integrity, and authentication. Where possible, the DSN is configured to minimize attacks on the system that could result in denial or disruption of service.



JITC and Command & Control issues

General and Military-Unique Requirements (con't)

- **Interoperable Service.** DSN is designed with the capability to permit interconnection and interoperation with similar tactical, federal government, allied, and commercial networks. All hardware and software in the network must be JITC certified as being interoperable.
- **NS/EP Compliant Service.** DSN complies with the requirements, priorities, and procedures established by the National Communication System (NCS) regarding national security and emergency preparedness (NS/EP). In the United States and its territories, NS/EP support is provided in accordance with Federal Communications Commission (FCC) rules and regulations through the commercial telecommunications industry and the Telecommunications Service Priority (TSP) system. For example, access to the Government Emergency Telecommunications Service (GETS) is available via the DSN. The DSN must comply with the NS/EP's TSP system for service restoration. Within the continental United States (CONUS), NS/EP TSP-approved requirements will be provisioned within 72 hours. In outside-CONUS (OCONUS) areas, not under the control of the US Government, DOD will provide NS/EP support where feasible and available through agreements with host governments and in accordance with TSP. OCONUS requirements will be provisioned as quickly as possible.

SAC Primary Alert Network C2

SAC Automated Command and Control System (SACCS) 465L System

VOIP desktop solution alternatives

- Softphone (Software)
  - turn any PC or laptop into a full-functioning telephone
  - Cost $50, Speakers, Microphone, Software
  - Costs less than $.03 minute

- IP-Phone (Hardware)
  - Replace traditional POT
  - Cost $150 and up
  - Additional Inside Service Plant

VOIP desktop solution alternatives (con't)
Call-signaling protocols

- **Session Initiation Protocol (SIP), defined by the Internet Engineering Task Force (IETF)**
  - SCCP (Skinny), --Cisco
- **H.323, defined by the International Telecommunications Union (ITU)**
  - that defines the protocols to provide audio-visual communication sessions on any packet network.

These two protocols basically do the same thing, and most VoIP devices use one or the other. Under the hood, the two protocols work differently to accomplish the establishment of a VoIP connection; SIP is ASCII-based, and H.323 is binary-based.

VOIP desktop solution alternatives (con't) ***Mitigations***

- If softphones are in use, then another VLAN should be created and all PCs with softphones should be placed on this VLAN. Traffic filtering rules should allow VoIP traffic between this VLAN and the IPT VLANs. VoIP traffic should not be allowed on the data VLAN. Similarly, general data traffic should not be allowed to the IPT server or IPT phone VLANs.

- If softphones are densely deployed throughout the network, it is not practical to have a data VLAN and a softphone VLAN. Instead, all PCs, whether or not they have softphones installed, should be placed in a data VLANs. Traffic should be filtered as described for the softphone VLAN in the previous paragraph.

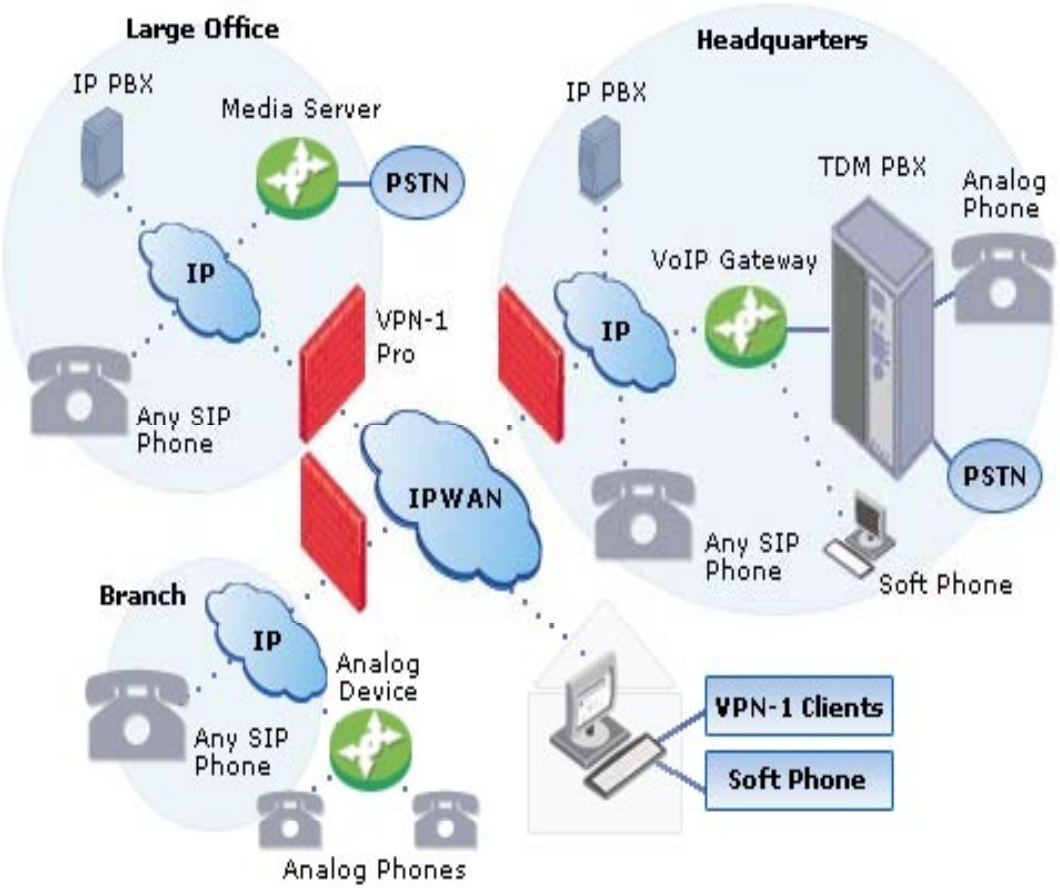
- When softphones are used as the primary voice communication mechanism, then a backup communication method, which does not depend on the PC, must be available in every office area.

Enterprise architectures convergence

Convergence (DISA)

- A VoIP network can be viewed as one logical switch in distributed form with the IP backbone providing connectivity to the distributed elements in the network.

- The IP infrastructure must ensure smooth delivery of voice and signaling packets to the VoIP elements.

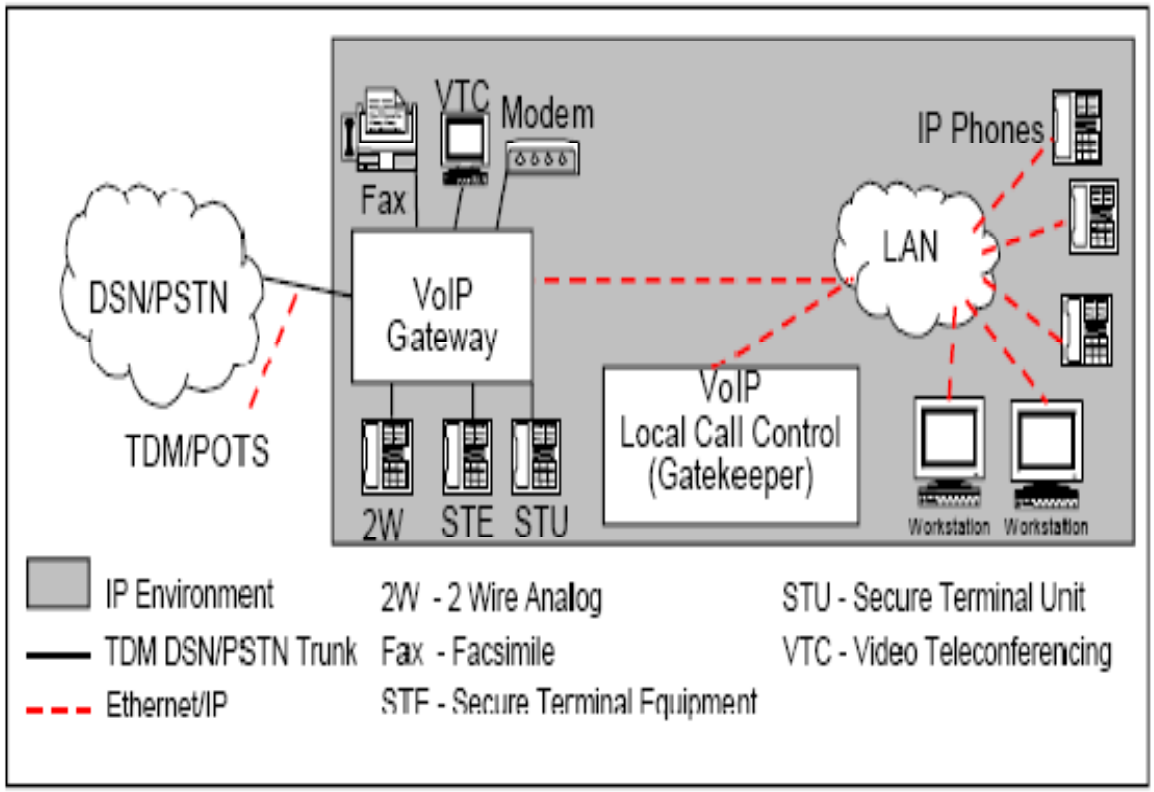


- If an IP network is to carry both voice and data traffic, it must be able to prioritize the different traffic types.

Enterprise architectures convergence

IP Centric (DISA)

- An IP Centric VoIP architecture is designed around an IP based core-switching system.
- Centric solutions have distributed IP devices that work together to perform the functions of a TDM based circuit-switch.



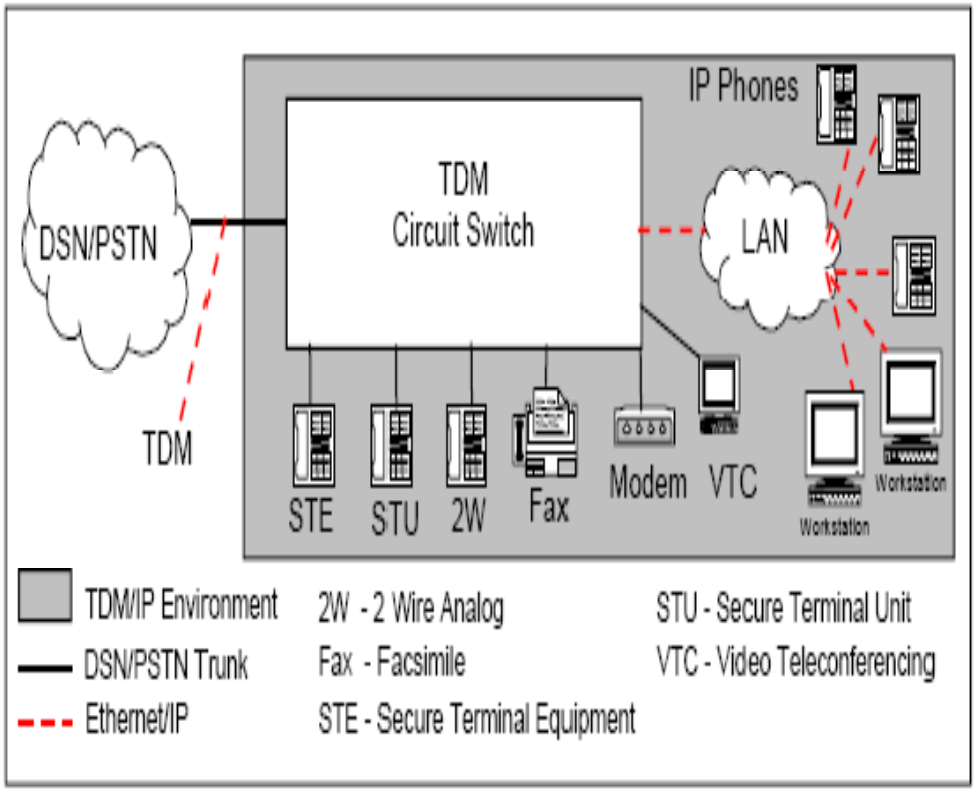
- IP centric solution connect to the rest of the switched network (i.e., TDM DSN/PSTN) via a dedicated trunk (i.e. T1/E1,or Integrated Services Digital Network (ISDN))equivalent.

Enterprise architectures convergence

IP Enabled (DISA)

- IP enabled architectures are considered hybrid solutions because they incorporate the services of a traditional TDM circuit-switch while providing VoIP terminals to the end subscriber.

- IP enabled solution use TDM based circuit-switch to provide the core call processing and switching.



  - The DSN/PSTN interface is provided via the TDM based circuit-switch. An integrated Ethernet interface provides connectivity to the IP Local Area Network supporting the IP Phones.

Enterprise architectures convergence
VoIP Threats

- VoIP Networks have many of the same threats to security, privacy and reliability as data networks do, but they also bring in the problems of the telephone system and have some special threats all their own.

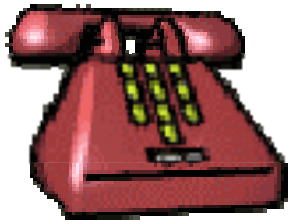
- Converged networks can combine threats from the data and VoIP world -- making the new network less secure (in the opinion of some).

- Data network people are afraid VoIP infrastructure will weaken the security of their data network and the voice/telecom people feel the same about data / IP networks.

Enterprise architectures convergence
VoIP vs. POTS
(Plain Old Telephone Service)

- Remember that “POTS” telephones have little security -- ordinary phone conversations are not encrypted and can be tapped or eavesdropped.

- You can actually have better security using VoIP via VLAN, VPN, DES3.



Enterprise architectures convergence
IP Network Threats

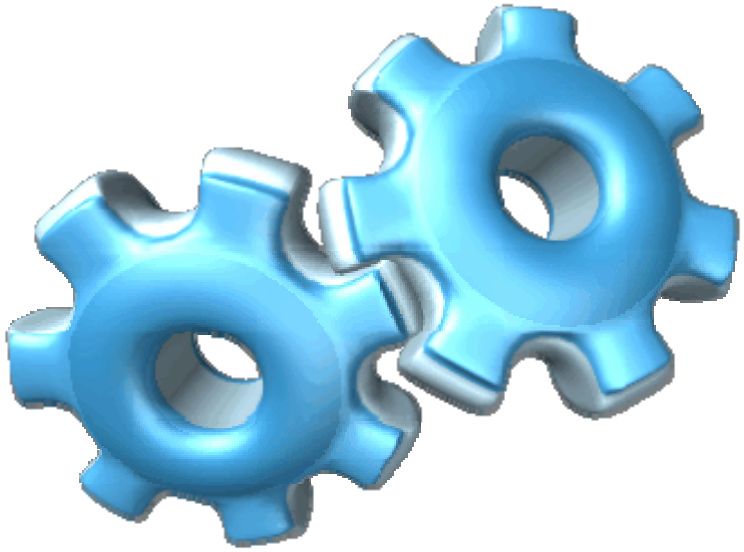
- Ethernet, IP and DNS address spoofing
- ARP and DNS Cache Poisoning
- Quantity-based packet flooding
- Stack DoS attacks
- VLAN “jumping”
- QoS / prioritization attacks

The next step – planning the move

- New C2 Definition needed for 21st Century
  - C2 vs Administrative
  - Secure Administrative IPT to replace 20th Century unsecure POT
  - Virtual IPT Networks extending to homeland security

- New DoD Framework
  - DWDM (dedicated wavelength for IPT)
  - WiMax (redundant network for IPT)

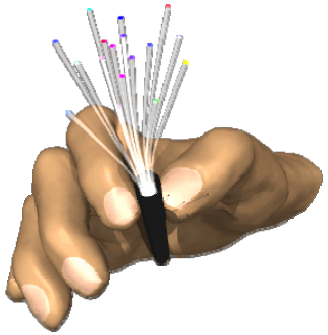
The next step – planning the move (con't)



- MILCONS
  - IPT only
- Next Gen DSN
  - Integrate current demonstration IPT projects
    - USN Pearl Harbor -3000 VOIP
    - JICPAC – 2000 VOIP
  - Change the transport model

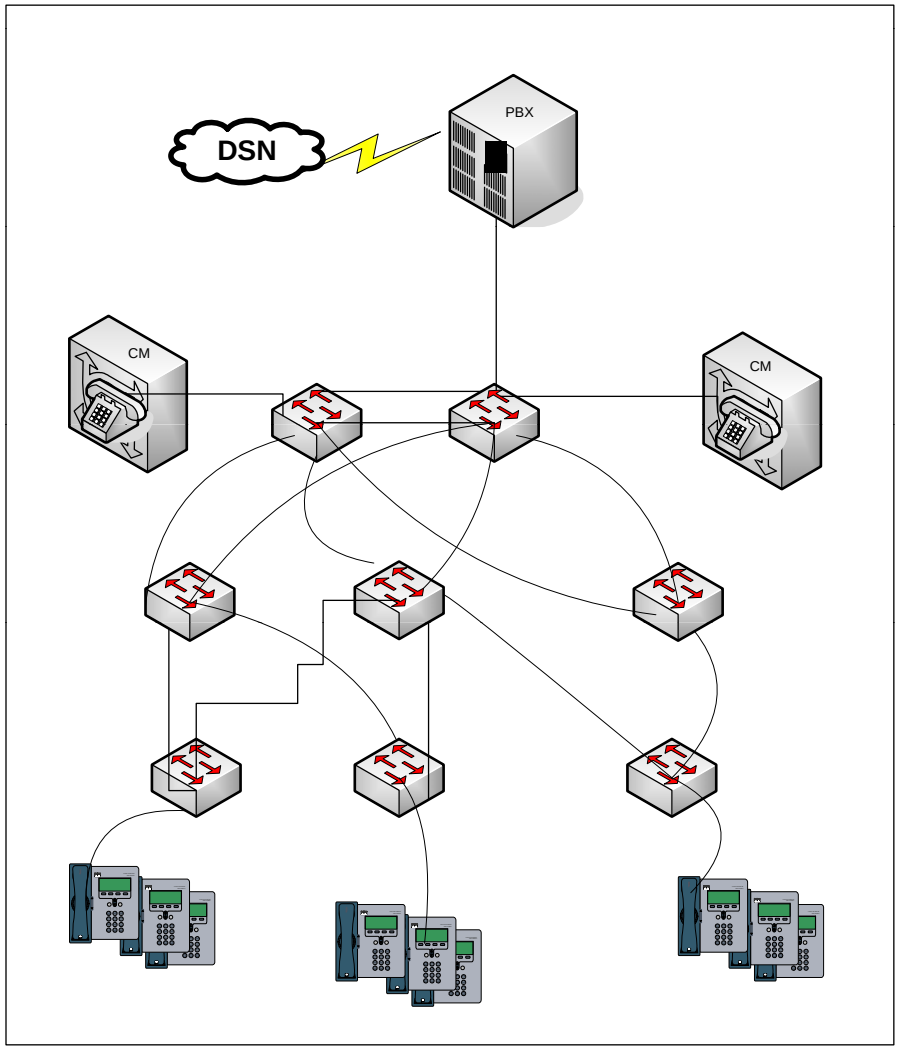
The next step – planning the move (con't)

- Phase OUT TDM
  - IPT only
  - BCO Techs the correct skill set to manage IPT systems
    - Lessons learned from deployment of IPT at AAFB, Guam
    - It is easier and more logical flow to train BCO tech on IP issues then to train IP Tech on Telephony. Capt Leuenburger, OPS, Andersen AFB, Guam
- Next Gen Telephony
  - BCO of the 20th century is going the way of the dinosaur
    - BCOs fighting battles each day for funding
    - BCOs need to design themselves in to extension
  - Industry must standardize ,Voice, Video, handsets protocols
- Joint Chief of Staff (JCS)
  - DISA/JITC deploy new model for IP services
    - Administrative vs. C2



Basic Solution

JITC Cert




QUESTIONS

Abbreviations

ARP	Address Resolution Protocol
BCO	Base Communication Office
DES3	Data Encryption Standard "Triple"
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoS	Denial-of-Service
DSN	Defense Switched Network
DWDM	Dense Wavelength Division Multiplexing
E1	European digital transmission format devised by the ITU-TS 2.048 Mbit/s
ISDN	Integrated Services Digital Network
IPT	IP Telephony
JICPAC	Joint Intelligence Center of the Pacific
JITC	Joint Interoperability Test Command
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
T1	US data circuit that runs at the original 1.544 Mbit/s line
TDM	Time-Division Multiplexing
VLAN	Virtual Local Area Networks
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access